



Voxogo ApS
Robocall Mitigation Plan
Pursuant to 47 CFR § 64.6305
Date: April 27, 2026

I. Introduction and Commitment

This Robocall Mitigation Plan is submitted by Voxogo ApS (the “Provider”), a voice service provider as defined in 47 CFR § 64.6300(l). It describes the specific reasonable steps the Provider has implemented to avoid the origination of illegal robocall traffic, consistent with 47 CFR § 64.6305(d)(2)(ii) and FCC Public Notice DA-24-73.

The Provider certifies that all calls originated on its network are subject to this robocall mitigation program. The Provider commits to:

- Taking affirmative, effective measures to prevent new and renewing customers from originating illegal calls.
- Responding fully to all traceback requests from the Commission, law enforcement, or the Industry Traceback Group (ITG) within 24 hours.
- Cooperating fully in any investigation or enforcement action.

The Provider has not been prohibited from filing in the Robocall Mitigation Database, and no prior certification has been removed by Commission action.

II. STIR/SHAKEN Implementation Status

The Provider has not implemented the STIR/SHAKEN authentication framework on any portion of its operations.

Basis for No Implementation: As a pure reseller, the Provider purchases numbers and origination services primarily from DIDWW Ireland Limited, which has implemented STIR/SHAKEN on PSTN calls. The Provider’s traffic benefits from this upstream authentication framework where applicable. The Provider relies on the upstream provider’s STIR/SHAKEN deployment, combined with its own robust customer vetting, contractual safeguards, monitoring, and “know-your-upstream” procedures (detailed below) to mitigate illegal robocall traffic. The upstream provider’s RMD filing details and contact information are maintained internally and available upon request.

III. Measures to Prevent New and Renewing Customers from Originating Illegal Calls

The Provider takes the following affirmative, effective measures (per 47 CFR § 64.1200(n)(4) and DA-24-73), with heightened scrutiny for international customers:

- Enhanced Know-Your-Customer (KYC) Vetting:
 - All prospective customers must provide government-issued photo ID, proof of physical address, business formation documents (if applicable), tax ID/EIN (or foreign equivalent), and contact details.
 - For international customers: Additional requirements include local business registration, website/domain verification, U.S. references, credit/background checks,

and review of public records. High-risk cases may require video verification or third-party due diligence. Suspicious applications are denied.

- Renewals trigger re-vetting, particularly for international customers.
- Service Agreements and Acceptable Use Policies: All agreements explicitly prohibit illegal robocalls and spoofing. The Provider may immediately suspend or terminate service for violations. International customers receive clear (possibly translated) notices.
- Number Validation and Usage Monitoring: Customers are limited to Provider-assigned numbers. Real-time validation ensures originating calls match assigned numbers. CDRs are monitored for anomalies (volume spikes, short-duration calls, sequential dialing, suspicious international patterns).
- Differentiated Treatment by STIR/SHAKEN Segment: Traffic on STIR/SHAKEN-enabled portions receives authentication where possible. Non-enabled portions receive stricter analytics-based blocking.

These measures significantly reduce the risk of illegal robocall origination.

IV. Know-Your-Upstream Provider Procedures

The Provider maintains “know-your-upstream provider” procedures:

- Primary upstream number provider: DIDWW Ireland Limited.
- The upstream provider is required to maintain its own robocall mitigation program, provide compliance attestations, and support traceback.
- The Provider monitors traffic patterns from the upstream relationship, conducts periodic reviews, and maintains 24/7 contact channels. Relationships are terminated or restricted if illegal activity is identified.

Current upstream provider details are maintained internally and available upon request.

V. Call Analytics Systems

The Provider uses DIDWW Ireland Limited with capabilities including:

- Real-time SIP analysis, reputation scoring, anomaly detection, and automated blocking.
- Enhanced alerts for international traffic and non-STIR/SHAKEN segments.
- Regular reports to adapt to emerging threats.

VI. Contractual Provisions

Customer agreements and upstream contracts require compliance with robocall rules, traceback cooperation, blocking/termination rights, and indemnification. These are actively enforced across all network segments.



VII. Traceback Response and Ongoing Mitigation Practices

Dedicated personnel respond to traceback requests within 24 hours. Practices include real-time monitoring (with differentiation by STIR/SHAKEN segment), rapid blocking of suspicious traffic (especially international), full cooperation with authorities, and periodic plan updates.

Appendix A: Contact Information

Primary Robocall Mitigation Contact

Name: Jakob M. Nielsen

Title: CEO

Phone: +4550506624

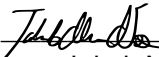
Email: Jakob@voxogo.com

24-Hour Traceback Email: Support@voxogo.com

Upstream Providers (if applicable): DIDWW Ireland Limited

Certification

I, the undersigned officer of Voxogo ApS certify under penalty of perjury that the foregoing is true and correct and that this Plan complies with 47 CFR § 64.6305(d).

Signature: 

Printed Name: Jakob Munk Nielsen

Title: CEO

Date: April 28, 2026